APPLICATION UNDER UNITED STATES PATENT LAWS

Atty. Dkt. No. __035817/0269919__
_____(M#)_____

Invention: ***"Automated Updating of Access Points in a Distributed Network"***

Inventor (s):   Francis M. Anton, Jr.

Pillsbury Madison & Sutro LLP
Intellectual Property Group
1100 New York Avenue, NW
Ninth Floor
Washington, DC 20005-3918
Roger S. Joyner (36,176)
Telephone: **(650) 233-4552**

This is a:

☐ Provisional Application

☒ Regular Utility Application

☐ Continuing Application
  ☐ The contents of the parent are incorporated
    by reference

☐ PCT National Phase Application

☐ Design Application

☐ Reissue Application

☐ Plant Application

☐ Substitute Specification
Sub. Spec Filed _____
     in App. No. ____/_____

☐ Marked up Specification re
Sub. Spec. filed _____
     In App. No ____/_____

SPECIFICATION

AUTOMATED UPDATING OF ACCESS POINTS

IN A DISTRIBUTED NETWORK

BACKGROUND OF THE INVENTION

5   ### 1. Field of the Invention

The present invention relates generally to distributed digital communication

networks, and more particularly to a system and method of automatically updating access point

devices in such networks.

10   ### 2. Description of Related Art

The popularity of the Internet has made a vast amount of information readily

available to anyone with an Internet connection. Internet-enabled electronic mail has become an

essential form of business communication. Currently, connections to the Internet are

predominantly made with landline access links such as dial-up modems, digital subscriber lines,

15   and cable modems.

These types of connections, although pervasive, offer limited mobility to a user

and make the sharing of an Internet connection difficult. For example, many libraries offer

Internet access at dedicated computer terminals and some universities provide network access

jacks at multiple buildings on their campuses for convenient access by students using laptop

20   computers. Both of these approaches offer a means for accessing the Internet at locations other

than one's own landline access link, but both require that one remain stationary at the publicly-

provided access point and both require a substantial infrastructure investment on the part of the

institution providing the network connection. Since it is not generally possible to have multiple

users sharing the same network access jack or dedicated terminal, the institution must provide a separate access point for each patron it wishes to service. Additionally, those institutions offering access jacks to their network, such as universities, typically require that the user have a registered network account before being given access to the network, which further limits the network's accessibility to the public.

Similarly, when a customer visits a service provider site on whose computer network the customer does not have an account, the customer will find it very difficult to gain access to the network, and hence to the Internet, email accounts, and other vital data. Should the customer be fortunate enough to gain access to a network jack, the customer will still be at the mercy of the service provider site network administrator. For security reasons, it is customary for service provider companies to set up their computer networks to deny access to anyone not already present in their access list of registered users.

Thus, mobile access to the Internet is limited by two factors. The first is the physical requirement for a user to maintain a line connection to sparsely located network access jacks. The second is the difficulty in gaining access to a network on which one does not have a registered account. The first of these factors has begun to be overcome by the introduction of wireless data networks, which do not require that a user maintain an access line plugged into a network access jack and thus do not require that the user remain stationary. Additionally, because the network connections are made wirelessly, it is relatively easy for multiple users to connect and disconnect from a network using the same access point. Overcoming the second factor is not so straightforward, and is addressed more fully below.

An example of a currently widely available wireless data network is the low speed personal communication service (PCS) network. The primary access devices of this type of

- 2 -

network are cellular telephones with built-in Wireless Application Protocol (WAP) features.

These wireless networks operate in a licensed frequency band, are centrally planned, and are

built by large telecommunication carriers. Typically, each cell has a large radius of about 2-10

miles and operates at a slow speed of about 19 Kbps. In any given geographical region there are

5   only a handful of telecommunication carriers servicing the area, and each network is proprietary

and closed to competing networks. Thus, to some degree one is not free to roam from one

network to another. Additionally, their slow speed makes full access to the Internet impractical

and such network devices are typically restricted to abridged textual displays.

An emerging new class of wireless data networks offer higher speeds of about 1 -

10   11 Mbps. These networks operate in an unlicensed frequency band and are based on emerging

wireless communication protocol standards such as IEEE 802.11, Bluetooth and homeRF. A

common characteristic of these types of networks is a small cell radius of about 200 feet. The

cells are radio or infrared base stations that function as access points to a network. Several of

these access points may be distributed in close proximity to each other to expand the overall

15   range of this type of wireless network. An introduction to such networks can be found in U.S.

Patent Nos. 5,771,462 and 5,539,824.

Various network configurations may be formed using these types of wireless

network devices. FIG. 1 shows multiple computers 11 to 17 equipped with wireless network

radio devices characterized by respective antennas 19 - 25. When computers 11 - 17 are within

20   close proximity to each other, they can form a type of ad hoc network and communicate among

themselves. Absent from this type of ad hoc network, however, is a base station cell that can

connect their ad hoc network to a wireline network having landline access to the Internet.

Therefore, this type of ad hoc network does not have access to the Internet.

- 3 -

With reference to FIG. 2, in order to access the Internet, one needs to gain access to a network having a router 37 which in turn connects the network to the Internet 35. These types of networks are typically characterized by a server 31 which controls access to various services on the network, including Internet services. Workstations 33 connect to the server 31 by

5   means of various types of hardware cabling media 53. The network may provide wireless access points 41 and 43 to respectively couple computers 47 and 49, which are equipped with wireless communication devices illustrated as antennas, to the hardwired network controlled by server 31. The access points 41 and 43 establish wireless connections with computers 47 and 49 by means of various communication systems such as radio and infrared waves, and have a hardwired

10   connection to server 31 along cable 53. The function of access points 41 and 43 is to relay communication between server 31 and wireless network computers 47 and 49 respectively, but server 31 still controls what services are provided to computers 47 and 49. Thus, server 31 may deny Internet services to computers 47 and 49. Indeed, server 31 may refuse computers 47 and 49 entry to the network if they do not already have network accounts registered with server 31.

15   As was stated above, wireless networks have a short range, and so a second access point 45 may be used to function as a repeater between a more distant wireless network computer 51 and access point 43. This is an example of using multiple base station access points 43 and 45 to extend the range of a wireless network.

With reference to FIG. 3, many network layout configurations are known, and

20   server 54 need not be located between a router 55 and the other network nodes 61 to 65. In the network layout of FIG. 3, access point 67 has direct access to router 55, which in turn has access to the Internet 59, but this does not mean that server 54 loses its control over the network. Regardless of the layout, server 54 may still be in charge of authenticating new users and

- 4 -

assigning resources. Again, access point 67 is illustrated as a wireless access point due to its convenience in permitting multiple users 61 to 65 easy access to the network, but other hardwired access point connections are likewise typical.

In spite of their convenience, such wireless networks have been prohibitive in the
5   past due to their relatively high costs. Until recently, the components required to implement a wireless network had been costly, but recent developments in technology have begun lowering the price of both the cell base stations and radio devices needed to implement a wireless network. Such wireless networks are now becoming more prevalent in the industry, and there may be a time when many small businesses may operate their own autonomous wireless networks. The
10   size of these autonomous wireless networks could range from a city block, to a small building, to a coffee shop. It would then be possible for a mobile user to always have access to a wireless network by means of a mobile computing device equipped with the proper radio communication devices. Thus, this type of wireless network would overcome the first factor limiting the free and mobile access to the Internet discussed above.
15   Nonetheless, one is still faced with the second factor mentioned above which restricts mobile access to the Internet. Since most autonomous wireless networks are independent, a mobile user would typically not be given access to a target network unless an access account had been set up ahead of time for the mobile user on the target network. Even if a user had access accounts at multiple wireless networks, the user would have to stop his
20   activities and re-authenticate on a different wireless network every time he moved from one autonomous network to another.

Some prior art can be found in the areas describing methods of accessing foreign networks and methods of implementing multiple network transfers. U.S. Patent No. 5,878,127,

- 5 -

for example, shows a telephone system that facilitates remote access to a private network from non-network locations or stations. The system authorizes remote access to the private network based on a calling party number of the non-network station and/or an authentication code entered by the remote calling party. U.S. Patent No. 6,016,318 describes various methods of providing

5 access to a private LAN and to the Internet via a "public mobile data network" including a location register, which serves as a database for storing location information of mobile data terminals and subscriber information. Along a similar note, U.S. Patent No. 5,978,373 shows a method by which a remote user can gain secure access to a private WAN. A central authentication office acts as a proxy to authorize a remote user and establish a secure connection

10 to the private network. The central office sends the remote user a service registration template HTML file to be filled by the remote user. Once the remote user has been authenticated, a connection is made with the private network. Similarly, U.S. Patent No. 5,918,019 shows a system by which a remote user can establish a simulated direct dial-up connection to a private network via the Internet.

15 U.S. Patent No. 6,000,033 describes a system wherein a user has accounts in multiple databases with different passwords in each of the databases. To access all of the databases, the user logs on to a master password database which then submits the appropriate password to whichever database the user wishes to access. U.S. Patent No. 5,872,915 shows a method of permitting secure access to software on a web server via the Internet. A user enters

20 data via a web browser, which is communicated to the web server application. The web server application then authenticates the web browser, and passes appropriate input data to an application gateway, including data to uniquely identify the web browser. The application gateway then uses authentication data received from the browser to determine whether the user

- 6 -

of the browser is authorized to access the software application. U.S. Patent 5,805,719 describes another method of authenticating a user wherein the system forgoes the use of ID tokens in favor of authorizing transactions by using the correlative comparison of a unique biometrics sample, such a finger print or voice recording, gathered directly from the person of an unknown user,

5   with an authenticated biometrics sample of the same type obtained and stored previously.

Referring again to FIG. 2, although the access points 41 and 43 may provide effective, high-speed connections between user devices and a landline network, the range of the equipment is typically limited and may be restricted to line-of-sight connections with user devices. For this reason, access points are advantageously placed in high traffic areas where they

10   can interact most easily with a large number of potential users. Typically, such locations are in public places where theft and vandalism may be a problem, or in places out of the way from public accesses. For this reason, access points are typically installed in high places to limit or eliminate casual access thereto. This, however, creates another problem — namely, it makes maintenance of the access points, such as repair of access point equipment and updating access

15   point software, more difficult.

SUMMARY OF THE INVENTION

The above described methods of authenticating a user and increasing communication between foreign networks do not provide for convenient maintenance of access

20   point equipment.

It is an object of the present invention to provide a system for maintaining access point devices in a communication network which permits easy access point software maintenance.

- 7 -

It is a further object of the present invention to provide a system for maintaining

access points in a communication network which permits easy access to software resident in

access points disposed in largely inaccessible places.

It is another object of the present invention to provide an access point system for a

5   communication network which can simultaneously provide a secure environment for access

points and a straightforward facility for modifying software in the access points.

It is yet another object of the present invention to provide an access point system

for a communication network which can automatically update itself to reduce the need for

manual maintenance.

10   In meeting the above objects, one aspect of the present invention provides a

method of permitting distributed access control of computing devices across a plurality of small-

radius data networks. The present invention, however, is not limited to small-radius data

networks, and can be applied to traditional hardwired, large-radius networks. A user wanting to

gain access to a private network first makes a physical connection to the target network. The

15   physical connection may be through a wireless base station, or may be through a wired hub,

switch, or firewall. Once connected, the potential new user may then try to gain access to the

target network's resources, such as Internet services.

Typically, a private network would respond to a new user attempting to gain

access to the network by first attempting to verify the new user's identity and network privileges.

20   If the new user is not among the private network's lists of authorized users, then the private

network would have the choice of refusing the new user entry to the network or establishing a

temporary session with minimal privileges for the new user under a guest account. If the new

user were given a guest account, however, the private network would not have an accurate record

- 8 -

of the new user's identity. Thus, most private networks choose to refuse entry to any

unregistered users. This type of network response is especially problematic in an envisioned

distributed network consisting of multiple small private networks responsive to mobile

individuals. The present invention seeks to alleviate this predicament by establishing a system

5   by which new users in such "guest" accounts would be accurately identified.

This identification is useful not only for maintaining an accurate log of all users

on a network, but also for billing purposes. For example, in a distributed network consisting of

multiple small private networks, it may be desirable to bill "guest" users for access time on a

private network. In the present invention, this is accomplished by having a centralized

10   authentication web server to which both a mobile user and a target private network subscribe.

The mobile user creates an account with the authentication web server, including an

identification means such as a password. The private network accepts the authentication results

from the authentication web server and creates the appropriate limited network access for the

new user.

15   In operation, a client device (new user) physically connects to the target network

via an access control device and initiates an Internet access request. If the client device is not

among the target network's list of authorized users, the access control re-directs the client device

to the authentication web server via the Internet. The authentication web server sends the client

device an HTML logon page through which the client device supplies the proper authentication

20   information to the system. The authentication device parses the information sent to it by the

client device and authenticates the client device. If the client device is properly identified, then

the authentication web server sends an "unblock" message to the access control device which is

used exclusively for the specified client device. All further traffic from the client device flows

- 9 -

through the access control device until an access expiration event happens, such as a timer

expiration, an explicit "disable client device" message, or a client device disconnected message.

It is thus very important that the authentication web server be able to accurately

identify both the client device and the target network. Due to the pervasive use of network

5   address translation services in the industry, it cannot be assured that the IP addressing

information received from the client device is accurate, nor would it be prudent to rely on

identification information from the web browser, such as cookies, to establish the identity of the

client device; otherwise the system would be susceptible to malicious use by software hackers.

Therefore, the present invention establishes the identity of users by using embedded IDs

10   generated from the client device's and access point's hardware host addresses into reserved string

fields of an HTML file.

Additionally, since the present invention is interested primarily in providing

Internet access to mobile users, the present invention proposes the use of enhanced remote access

points having built-in router capabilities to directly connect a potential client user to the

15   authentication web server and the Internet without the need of a private party's autonomous

network. The authentication web server would maintain a record of the individual access points

used and the names of the client users. Thus, the owners of the enhanced access points would

still maintain an accurate record of all users for billing purposes. Alternatively, the client users

could be billed or charged directly by the authentication web server and a percentage of the

20   billings sent to the owner of the enhanced access point used by the client user.

Other objects, as stated above according to an aspect of the present invention are

achieved by providing self-maintaining access points. In addition to conventional access point

functions such as facilitating communications between wireless-enabled portable devices and a

- 10 -

communications network connected to the access points, these self-maintaining access points are additionally able to overwrite software stored therein with new software received via the communications network. Thus, maintenance, upgrading and replacement of access point software can be done without physically accessing the access points. This means that physical

5   access to such inaccessibly-mounted access points can be limited to hardware maintenance such as equipment upgrades, replacements and the like.

The present invention includes a method and system for maintaining network access point equipment including installing and upgrading software. The system includes a network server and access point equipment including one or more access point devices, with

10   each device equipped with a CPU including a random access memory (RAM) and a programmable read only memory (PROM). The server is configured for receiving software for maintaining the programming of access point devices. Both the access point devices and the server are programmed with authentication software for identifying each other prior to transmission of maintenance data. The access point devices are further programmed to

15   periodically do a software check with the server. If the current software version in the device is the same as that stored in the server, no action is taken. If the version in the server is different, then the system automatically loads the current software version into the device.

BRIEF DESCRIPTION OF THE DRAWINGS

20   These and other objects, features and advantages of the present invention are better understood by reading the following detailed description of the preferred embodiment, taken in conjunction with the accompanying drawings, in which:

- 11 -

60212037V1

FIGURE 1 is a prior art depiction of an ad hoc network using wireless communication;

FIGURE 2 is a first prior art network layout using both wireline and wireless network connections;

FIGURE 3 is a second prior art network layout using both wireline and wireless network connections;

FIGURE 4 is a prior art depiction of network communication using IP protocols;

FIGURE 5 is a prior art depiction of the use of network address translation;

FIGURE 6 is a first network layout in accord with the present invention;

FIGURE 7 is a second network layout in accord with the present invention;

FIGURE 8 is a block diagram of message flow in the first network layout;

FIGURE 9 is a block diagram of the system of the present invention; and

FIGURE 10 is a flow chart of the method of the present invention.

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS

In order to facilitate the use of the present invention, the best mode of a presently preferred exemplary embodiment makes use of existing hardware and software tools with minimal modification to both. As it is known in the art, network communication processes are divided into multiple standardized stages, or layers, and each layer is assigned a specific task necessary for network communication. A widely used network communication standard is the Open System Interconnection (OSI) standard developed by the International Standards Organization (ISO). The OSI communication model divides network communication into seven layers. Each layer has a predefined, standardized mechanism for communicating with the layer

- 12 -

immediately above it and immediately below it. In this manner, any layer may be modified or optimized without requiring modification of any other layer as long as the same standardized mechanism is used to communicate with adjacent layers.

The first layer is the physical layer and it describes the hardware medium for transmitting and receiving a logic 1 and a logic 0. The second layer is the data link layer and it translates messages into correct format for the physical layer to transmit, and translates messages received by the physical layer for upper layers to understand. Basically the data link layer formats messages into data frames that encapsulate the messages and adds customized information, including a CRC code, destination address information, and source address information. The third layer is the network layer and its main function is to direct data from a source network to a destination network. This third layer is sometimes called the Internet layer since its job is basically to route messages and provide a standard network interface for upper layers. The present invention preferably resides in this third layer, and thereby can be implemented with software modifications without requiring any additional hardware modifications. Since much of the existing hardware, such as routers and hubs, have updateable firmware, the preferred embodiment of the present invention may be easily assimilated into current networks.

Various types of network protocols may be associated with the third layer of the OSI model, but the present invention preferably makes use of the Internet protocol, IP, which is the protocol used by many networks to communicate with the Internet. It may therefore be advantageous to briefly describe further aspects of the IP addressing protocol relevant to the best mode of the preferred embodiment of the present invention before proceeding further in this discussion.

- 13 -

With reference to FIG. 4, computer 71 is part of a first network 72 wishing to communicate with computer 75, which is part of a second network 79. The two networks 72 and 79 are coupled by router 74, which relays messages between the networks 72 and 79. Every node in a network has a unique hardware address, including side A of router 74, which communicates with computer 71, and side B of router 74, which communicates with computer 75. When nodes within the same network target each other for communication, the sent messages are encapsulated with header information including the hardware and IP address of the source node and the hardware and IP address of the destination, or target, node. All nodes within the same network may pick up the message, but the message is ignored if the destination hardware address does not match their own. If the hardware address does match a particular node, then that node checks the IP address of the message to verify that they are indeed the intended receiver of the message. For example, if computer 71 wished to send a message to router 74, then the message header would include a source hardware address of 100, source IP address of 222.222.222.1, a destination hardware address of 200 and destination IP address of 222.222.222.2. If router 74 wanted to respond to the message then its response would include a similar header with the source and destination addresses interchanged.

When messages must pass several networks to reach their destination node, the header information changes every time the message traverses a router. Nonetheless, the IP address of the destination node is maintained constant across the networks. As an example, assuming that computer 71 wishes to send a message to computer 75, the header of the information must relay the message through router 74. Therefore, the message leaving computer 71 will include a source hardware address of 100 and an IP address of 222.222.222.1, as well as the IP address of computer 75. However, since computer 75 is not within the same network as

- 14 -

computer 71, the message will include the hardware address 200 of the router 74. The router 74 will pick up the message since the message has its hardware address, but upon inspection of the destination IP address will determine that the final destination is that of computer 75. Therefore, the router will forward the message to computer 75 with a new header. The new header will

5   identify computer 71 as the originator of the message by maintaining its source IP address of 222.222.222.1, but will identify router 74 as the sender of the forwarded message by listing the source hardware address 300 of side B of router 74. Since side B of router 74 faces the same network 79 as computer 75, the forwarded message will include the correct destination hardware and IP address of computer 75. When responding, computer 75 will know that the original

10   source of the message was computer 71 because its IP address was preserved in spite of having received the message from the router 74. This would be true no matter the number of routers the message had to traverse before reaching computer 75. In this case, it can be seen that the source IP address in the header of a message can uniquely identify the originator of a message, whereas the source hardware address changes every time the message passes through a router and is thus

15   not a reliable source for identifying the originator of the message. It would seem therefore that the source IP address in the header of a message would be a prime candidate for identifying a specific node across multiple networks, as is required by the present invention. However, this is not the case if a message crosses a network making use of Network Address Translation (NAT) services to manage its access network nodes.

20   In order for a node to access the Internet, the node must have a unique IP address. However, the number of unique IP addresses is limited and many networks make use of NAT services for permitting many network nodes, or network computers, to access the Internet using the same IP address.

- 15 -

A simple example of network address translation is shown in FIG. 5. Here, computers 73, 77 and 81 are part of a network that shares a single valid IP address, 201.1.2.3, by means of a network address translation manager 78. Each of computers 73, 77 and 81 is given an arbitrary IP address that is unique within the network, but is not necessarily a valid Internet IP

5 address. When any of computers 73, 77 and 81 wants to access the Internet 80, they must first go through NAT manager 78, which relays the message to the Internet with the correct IP address 84 and its own hardware address 104. Additionally, NAT 78 assigns a unique access port number to each incoming message from computers 73, 77 and 81, and maintains a table associating the hardware and IP address of the originating source computer 73, 77, 81 with the

10 assigned port number. This assigned port number is part of the identification data included in the header encapsulating a message, and is therefore sent along with the message to the Internet 80. When a message is received from the Internet 80, the header information of the received message will list the IP and hardware address of NAT 78 as its destination data, but will also have the port number NAT 78 had assigned to the originally relayed message. NAT 78 uses this port number

15 to identify which of computers 73, 77, 81 originated the message and relays the response from the Internet to the computers 73, 77, 81 accordingly.

Thus in this case, a target web page within the Internet 80 will not be able to identify the originator of a message since all messages coming from the network behind NAT 78 will have the same source IP and hardware address. Therefore, this preferred embodiment of the

20 present invention chooses not to rely on the source IP address in the header of a message when trying to identify the network node that originated a message.

An object of the present invention is to be able to uniquely identify a mobile user no matter what type of network the user connects to in order to gain access to the Internet.

- 16 -

Therefore, a preferred embodiment of the present invention deviates from the prior art when identifying the source of a mobile user.

A first embodiment of a network system in accord with the present invention is shown in FIG. 6. The present invention may be utilized in a network having a layout similar to that of FIG. 2 or any other known network configuration, but it is preferred that an access point 123 in accord with the present invention be placed close to a network node with Internet access. In FIG. 6, router 127 couples a source network 129 with the Internet 131. Therefore, access point 123 is shown next to router 127. In the present example, a mobile user utilizing a laptop computer 121 connects to network 129 using wireless access point 123. It is to be understood that a mobile user may also connect to network 129 by means of a hardware access jack.

Within network 129, server 125 is preferably in charge of authenticating all new users and allocating various network services, including Internet access. In the present example, the mobile user accesses network 129 using a laptop computer 121 and access point 123, but does not have a network account with server 125 and would therefore typically be denied network access. Nonetheless, the mobile user initiates an Internet access session to a desired target web page 133 by means of almost any web browser, such as Microsoft Internet Explorer, Netscape Navigator, etc. The mobile user device 121 thus goes through its domain name resolution process to identify the address of target web page 133. Network 129 will permit all DNS traffic to the Internet, even from an unauthorized user, and the mobile user thus receives the correct IP address of its target web page 133.

As is known in the art, a TCP connection is started by a source host sending a SYN, i.e., synchronize/start, packet to a destination host and then waiting for a synchronize acknowledge (SYN ACK). In the present case as shown in FIG. 8, however, when mobile user

device 121 attempts to open an HTTP connection to the target device 133 by sending a TCP SYN packet to the target web page 133 using the acquired destination IP address in Step 1, a source network 129 server, indicated in FIG. 8 by the Network 129 block, intercepts the packet and checks if the mobile user device 121 is authorized to gain access to the Internet. If it is, then the message is forwarded accordingly. If the mobile user device is not authorized, then the packet is re-routed to a predetermined redirection web server 139. Redirection web server 139 responds in Step 2 by transmitting a "Web Site Relocated" message that points the mobile user device 121 to an authentication web server 137 (this redirection ability is conventional to HTML, a common language for encoding web pages). The mobile user's web browser responds to the "Web Site Relocated" message by automatically re-sending the HTTP request to authentication web server 137 in Step 3. Again, network 129 intercepts the TCP SYN packet, but upon recognizing that the target website is now the authentication web server 137, the packet is forwarded without alteration.

Thus, network 129 does not prohibit Internet access by unauthorized users, it merely restricts it to a limited number of predetermined websites. Internet access requests to a preauthorized website, such as authentication web server 137, are permitted access to the Internet, but all Internet requests to unauthorized websites are automatically re-routed to redirection server website 139.

In Step 4, authentication web server 137 presents the mobile user device 121 with an HTTP form page soliciting authentication information from the mobile user. The user-supplied authentication information may include a user ID and password, which the user enters via his web browser. At this point, it should be noted that although the mobile user ID has been given an IP address by network 129 in order to communicate within the network, the Internet

- 18 -

packet transmitted from the mobile user device 121 to authentication web server 137 may not be relied upon to uniquely identify mobile user device 121 because of the possible use of network address translation by network 129. To overcome this limitation, the HTTP form page transmitted to the mobile user device 121 includes an embedded reserved field preceded by a

5   unique client device ID keyword EF1 provided by the authentication web server 137. The reserved field may be located within the out-going data packet a predetermined number of bytes away from the unique client device ID keyword EF1. Alternatively, the reserved field may be immediately preceded by the unique client device ID keyword EF1.

When the mobile user device 121 forwards its authentication data to

10   authentication web server 137 in Step 5, network 129 detects that a message packet is being sent to authentication web server 137 and responds by inspecting the message packet to detect the embedded reserved field. Since the message has come directly from mobile client device 121, its unique hardware address in the header of its message packet is still valid. Network 129 responds by generating a new client device ID keyword EF2 based on the unique hardware address of

15   mobile client device 121, the current session information, and the address information of network 129. This address information will be dependent on the device on which the present system is implemented. This new client device ID keyword is inserted into the embedded reserved field and the modified message is forwarded to the authentication web server 137 in Step 6.

20   Upon receiving the HTTP form page from user mobile device 121, authentication web server 137 parses the information in the HTTP form page. Preferably, the information is parsed using a backend CGI script. The authentication web server 137 forwards the user-supplied information and the new client device ID keyword from the embedded reserved field to

- 19 -

a gate keeper server 135 in Step 7. The gate keeper server may be accessed via the Internet, or may be directly connected to the authentication web server 137. Preferably, the information is transmitted from the authentication web server 137 to the gate keeper server 135 along a secured link.

5   It should be noted that server 125, redirection web server 139, authentication web server 137 and gate keeper server 135 need not reside on separate machines, and one or more of these may be co-resident on a machine. Further, these need not be servers in the usual sense of the word and may instead be web pages, scripts, applets or other routines capable of performing the attributed functions. Additionally, the functionality of redirection web server 139 need not

10   be separate and may be integrated into the network 129.

          The gate keeper server 135 processes the received authentication data information and checks if the user is registered. If the mobile client has a legitimate account, then the gate keeper server 135 decodes the new client device ID keyword that is in the embedded reserved field to determine the hardware address of the mobile user device 121. The gate keeper server

15   135 then sends an encrypted "unblock" message in Step 8 based on the same client device ID keyword to network 129. As explained above, the controlling device within network 129 on which the present system is running had inserted the address information of mobile user device 121 in the HTTP form page, therefore gate keeper 135 sends the "unblock" message directly to this controlling device. Preferably, the "unblock" message is encrypted with the new client

20   device ID keyword. Alternatively, a third client device ID keyword may be generated and used for the encryption process. It may include the hardware address of the mobile client device 121, as well as the Internet protocol address of the network 129.

- 20 -

Network 129 verifies the encrypted "unblock" message, and then updates its internal access list to grant Internet services to the mobile client device 121. All subsequent traffic from the mobile client device 121 to the Internet are forwarded by network 129 unimpeded until either an allowed access time expires as described in greater detail below, an

5 explicit "Disable client device" message is received, or the client device 121 disconnects from network 129.

In the description of FIG. 6, the present invention is described as a program routine running in network 129, but the location of the program routine was not explicitly stated. The present invention may be a program routine running in server 125, router 127 or access point

10 123, or parsed to have its routines distributed among all three.

Thus, all mobile users on network 129 are uniquely identified and verified. It is then possible for network 129 to charge a mobile user for access time on network 129. Alternatively, since the mobile user is authenticated by the gate keeper server 135, it may be advantageous that the gate keeper server 135, or another specialized server record the amount of

15 time that mobile user device 121 spends accessing the Internet 131 through network 129, and charge accordingly. In still an alternate embodiment, a mobile user will have already paid in advance for a predetermined amount of network access time as noted above. When a mobile user is admitted access to a private network, such as network 129, the amount of time paid in advance is transmitted to network 129, which then disconnects mobile user 123 once the time has

20 expired. Any remaining time not used by mobile user device 123 may be forwarded to the gate keeper server 135, or the corresponding specialized server, and the remaining time on the user's account may be updated accordingly.

- 21 -

An alternate embodiment of the present invention is shown in FIG. 7. Elements in FIG. 7 similar to those of FIG. 6 have similar reference characters and are described above. In the present alternate embodiment, access points 105 and 111 have routing capabilities for connecting to the Internet 131. Thus neither of access points 105 or 111 require a separate

5   hardwired network, such as network 129 shown in FIG. 6, to implement the present invention.

For illustrative purposes, wireless access point 105 is shown located in a coffee shop and wireless access point 111 is shown located in the waiting room of an automotive mechanic's shop. Mobile users may then access the Internet 131 via wireless access point 105 and any known device for establishing a node connection to a network, such as a handheld

10   computing device 101 or laptop computer 103. In the present example, access point 105 is shown as a wireless access device, but it may also provide hardwired connections to client devices. Similarly, a mobile user may use laptop computer 109 to access the Internet 131 via wireless access point 111. In this embodiment, it may be preferable for gate keeper server 135 to maintain a record of Internet access time by devices 101, 103 and 109, and then to send a

15   summary report to the owners of wireless access points 105 and 111.

Referring now to FIG. 9, a system 141 according to the present invention is illustrated in block diagram form. An access point device 143, such as items 105 and 111 in FIG. 6, is configured with a processor 145, a programmable read only memory (PROM) 147, and a random access memory (RAM) 149. The access point 143 is configured for communication

20   through a network 151, including communication with a server 153. FIG. 9 also shows a computer 155 having access to a network 157.

The system 141 includes programming for the purpose of providing an automatic upgrading of access point software 159 stored in the RAM 149. In general, the access

- 22 -

point management software has a first portion or portions that do not require upgrading which

are stored in the PROM 147. The portion or portions of the management software that may

require upgrading 159 are stored in the RAM 149, and include the currently loaded version of

access point management software (b), and access point wireless software (a), such as software

5   implementing the well known IEEE 802.11b protocol for managing wireless communication

between the access point 143 and mobile computers such as 47 and 49 of FIG. 2.

In one embodiment of the invention, the PROM 147 includes session

communication and management functionality using, for example the basic TCP/IP protocol,

software for authenticating the access point to the server and server to the access point, loading

10   software, controller/management software, and version check software. Similarly, the server 153

memory 161 includes authentication software for assuring that communication is from a

particular access point. Also, FIG. 9 shows only one access point 143, but the invention also

includes any number of access points, servers 153 and computers 155, for communication in any

number of networks 157. Further, it should be apparent that different types of memory other

15   than PROM 147 and RAM 159 may be employed, as well as different types of storage media as

will be understood by those skilled in the art. Still further, it should be apparent that the various

types of software may be divided among those different types of memory in other ways.

Moreover, software for implementing other functionality not necessary for the invention may

also be provided, but is not shown for clarity.

20   The facility for wireless communication is indicated symbolically in FIG. 9 by

transceiver (XCVR) block 163 and antenna 165.

In operation, a technician can enter a new version of access point 143 software

into the memory 161 of server 153. This may be done by manually accessing the server 153 and

- 23 -

providing a diskette, etc.; by downloading the software from a vendor, development department or the like; or other means. The access point 143 is programmed to automatically and periodically (e.g. once a day) shut down normal operation and check with the server 153 to ascertain the current version of access point software loaded in the server memory 161 *[Is it*

5   *necessary to shut down operation? Which is preferable?]*. If the current version 167 in the server 153 memory 161 is not the same as the version 169 in the access point 143, the access point 143 loads the current version 167 into RAM 149, replacing the old version. This automatic, periodic upgrading process avoids the need to physically access the access point sites, such as items 47 and 49 at FIG. 2, which as explained above may be in remote and difficult to

10   access places.

The programming of the access point 143 and server 153 will now be explained in reference to the flow chart of FIG. 10. The description assumes that the access point 143 is initially in a normal operational mode, processing communication to and from mobile, wireless equipped computers such as 47 and 49 (FIG. 2) or 155 (FIG. 9). This normal "run" state is

15   indicated in FIG. 10 as Step 171. The access point 143 is programmed to communicate with the server 153 at a pre-determined time, e.g., daily. This communication includes authenticating that the communication is occurring with the desired server 153. The server also can be programmed to authenticate that the communication is with a valid access point 143. These operations are indicated by Step 173. Once the communication link is established, the access point 143

20   activates a "version checker" program which requests and receives a version code from the server indicating the current version 167 of access point 143 management software loaded into the memory 161 of the server 153. The access point 143 processor 145 compares the version 167 from the server 153 with the version 169 in the access point 143 RAM 149 (Block

175). If the versions 167 and 169 are the same in Block 177, then the access point 143 returns to normal run operation via Block 179. If the version 167 in the server 153 is different from the version 169 in the access point 143 (Block 181), the access point 143 begins a shutdown operation 183. The access point 143 stops making new connections, and waits until all current connections are terminated (Block 183). When all connections are terminated the access point 143 continues (Block 185) and loads (Block 187) the new version 167 of the access point software from the server memory 161 into the access point 143 RAM 149, replacing version 169. When the new version is loaded into RAM 169, the access point 143 returns to normal "run" operation (Block 171).

The present invention has been described above in connection with a preferred embodiment thereof; however, this has been done for purposes of illustration only, and the invention is not so limited. Indeed, variations of the invention will be readily apparent to those skilled in the art and also fall within the scope of the invention.